Deutscher Bundestag **Drucksache 18/11401**

18. Wahlperiode 07.03.2017

Vorabfassung - wird durch die lektorierte Fassung ersetzt.

Antrag

der Abgeordneten Jan Korte, Frank Tempel, Dr. André Hahn, Katrin Kunert, Petra Pau, Martina Renner und der Fraktion DIE LINKE.

Datenschutzrechte der Bürgerinnen und Bürger stärken

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Das Alltagsleben, die Arbeitswelt und die öffentliche Verwaltung werden mehr und mehr von der Nutzung informationstechnischer Systeme durchdrungen. Allein durch die Nutzung des Internets fallen große Mengen personenbezogener Daten an. Dies stellt eine besondere Herausforderung für den verfassungsmäßig garantierten Schutz des Grundrechts auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dar.

Mit der Verabschiedung der Datenschutz-Grundverordnung (DSGVO, Verordnung (EU) 2016-679) haben die Regierungen der EU-Staaten und das Europäische Parlament einen Versuch unternommen, die bestehenden EU-Datenschutzregelungen den geänderten technischen Rahmenbedingungen anzupassen. Ausdrückliches Ziel war dabei bedauerlicherweise nicht allein, die Grundrechte der EU-Bürgerinnen und –Bürger zu schützen, sondern zugleich den Handel und die Verwertung von Daten innerhalb des EU-Binnenmarktes zu befördern.

Die Bundesregierung hat im Februar 2017 den Entwurf eines Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) vorgelegt, der zurecht auf teils massive Kritik von Datenschützern und Verbänden getroffen ist.

In zentralen Punkten – insbesondere bei den Betroffenenrechten – werden die Vorgaben der DSGVO aufgeweicht. Es bleibt weitgehend den Behörden überlassen, wie weit sie Bürgerinnen und Bürger über die über sie gespeicherten Informationen Auskunft erteilen. Auch Unternehmen können die Auskunft über die Speicherung und Verarbeitung von Daten verweigern, wenn „die Information die Geschäftszwecke des Verantwortlichen erheblich gefährden würde“ (§31 Abs. 1 Nr. 2 Bundesdatenschutzgesetz – Entwurf). Damit werden Geschäftsinteressen grundsätzlich über den Schutz persönlicher Daten gestellt, der durch die Auskunftsrechte erst durchgesetzt werden kann. Im Bereich der Patienten- und Sozialdaten soll es zukünftig keine Datenschutzkontrolle mehr geben, wenn davon Berufsgeheimnisträger betroffen wären. Derzeit ist dies ein Schwerpunkt der Datenschutzkontrolle durch die Aufsichtsbehörden in den Bundesländern.

Auch bei den Durchsetzungsmöglichkeiten der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) mangelt es an effektiven Mitteln,

teilweise sind sogar Einschränkungen gegenüber der derzeitigen Rechtslage vorgesehen. Im Bereich der Nachrichtendienste lässt der Gesetzesentwurf die längst überfällige Einführung einer unabhängigen Datenschutzkontrolle vermissen. Dies ist mit der Rechtsprechung des Bundesverfassungsgerichts nicht vereinbar. Die Beschränkungen der Prüf- und Berichtsbefugnis der BfDI im Geheimdienstbereich und die Beschränkung der Sanktionsmöglichkeiten der BfDI in den Bereichen Polizei und Justiz sind nicht nachzuvollziehen und daher nicht hinzunehmen.

Insbesondere den Beschäftigtendatenschutz gilt es an die digitalisierten Arbeitsprozesse anzupassen. Arbeitnehmerinnen und Arbeitnehmer müssen davor geschützt werden, zu Objekten vollständiger Überwachung und permanenter Leistungskontrolle degradiert zu werden. Die bisherigen Regelungen reichen dazu nicht aus.

II. Der Deutsche Bundestag fordert die Bundesregierung auf, einen Gesetzentwurf vorzulegen, mit dem

1. die Betroffenenrechte im Bereich des Datenschutzes gestärkt werden, indem auf Beschränkungen der Auskunftsrechte gegenüber öffentlichen und nichtöffentlichen Stellen - so weit im europarechtlichen Rahmen möglich – verzichtet wird und die Möglichkeiten ausgeweitet werden, personenbezogene Daten löschen zu lassen;
2. die Kompetenzen der BfDI gestärkt werden und zur effektiven Durchsetzung des Datenschutzes auch gegenüber öffentlichen Stellen Sanktionsmöglichkeiten geschaffen werden;
3. die unabhängige datenschutzrechtliche Kontrolle der Nachrichtendienste sowie Kontrollbefugnisse und Sanktionsmöglichkeiten der Datenschutzaufsichtsbehörden ausgebaut werden;
4. die im Rahmen so genannter Scoring-Verfahren verarbeiteten personenbezogenen Daten auf ein Minimum begrenzt werden und generell die Verarbeitung personenbezogener Daten insbesondere dann restriktiv gestaltet wird, wenn Daten zu anderen Zwecken verarbeitet werden, als sie ursprünglich erhoben wurden;
5. der Beschäftigtendatenschutz in einer eigenen gesetzlichen Regelung deutlich verbessert und den aktuellen Herausforderungen angepasst wird und
6. es den Datenschutzbeauftragten von Bund und Ländern anheimgestellt wird, wie sie ihre Vertretung im Europäischen Datenschutzausschuss selbst bestimmen wollen.

Berlin, den 7. März 2017

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion

Begründung

Die zunehmende Bedeutung des Internets in allen Lebensbereichen birgt viele Chancen, aber ebenso Risiken. Hackerangriffe auf Unternehmen und private Personen gefährden die freie Bewegung im Internet. Aber auch die massenhafte Erfassung, Speicherung und Auswertung von Daten über das Nutzerverhalten im Netz, stellt eine Gefahr für das Recht auf informationelle Selbstbestimmung dar, egal ob sie von Unternehmen oder staatlichen

Vorabfassung - wird durch die lektorierte Fassung ersetzt.

Überwachungsprogrammen ausgeht. Dies ist nicht nur eine Gefahr für jeden Einzelnen, sondern für die Gesellschaft als Ganzes. Unbeobachtete und freie Kommunikation sowie der ungehinderte Zugang zu Informationen sind zentrale Elemente einer demokratischen Gesellschaft.

Die EU-Datenschutzgrundverordnung (DSGVO) versucht diese Problematiken aufzugreifen und durch eine Harmonisierung weitgehend einheitliche Datenschutzvorschriften in der Europäischen Union zu erlassen. Doch der Entwurf eines Gesetzes zur „Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (Datenschutzgrundverordnung) und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz)“(DSAnpUG-EU-Entwurf) verfehlt diesen Anspruch. Denn der Entwurf wird den Datenschutzstandard in Deutschland, sowohl im Verhältnis zum Status quo als auch zur DS-GVO, deutlich absenken und das Recht auf informationelle Selbstbestimmung unangemessen einschränken. Die Bundesregierung riskiert mit ihrem unausgereiften Entwurf außerdem ein Scheitern der gesetzlichen Regelung vor dem Europäischen Gerichtshof. Die Deutsche Vereinigung für Datenschutz weist in ihrer Stellungnahme vom 01.02.2017 darauf hin, dass insbesondere die auch inhaltlich viel zu unbestimmte Einschränkung von Auskunftsrechten gegenüber öffentlichen und nicht-öffentlichen Stellen im § 29 des Entwurfs verfassungs- und europarechtswidrig ist.

Insbesondere im Anwendungsbereich der Datenschutz-Richtlinie 2016/680 für den polizeilichen Datenaustausch (§§ 45 – 84) lässt der Gesetzesentwurf die Rechtsprechung des Bundesverfassungs-gerichts zur Zweckbindung und datenschutzrechtlichen Kontrolle unberücksichtigt (BVerfGE 65, 1). Die Zweckbindung bei der Verarbeitung personenbezogener Daten muss demnach grundsätzlich erhalten bleiben, wobei in Ausnahmefällen eine Änderung der Verarbeitungszwecke mit dem Ursprungszweck vereinbar sein müssen bzw. diesen nicht unterlaufen dürfen. Im Bereich der DSGVO ist der Zweckbindungsgrundsatz ohnehin weitgehend ausgehöhlt, eine Weiterverarbeitung von Daten kann allein mit dem „berechtigten Interesse“ an der Verarbeitung begründet werden.

Umso wichtiger wäre ein weitgehendes Auskunftsrecht über die eigenen Daten. Die durch den Gesetzesentwurf geschaffenen Einschnitte in die Betroffenenrechte stellen jedoch in erster Linie eine Arbeitserleichterung für die Daten verarbeitenden Stellen dar, widersprechen aber dem Recht auf informationelle Selbstbestimmung. Beispielsweise schmälern Ausnahmen in der Informationspflicht aufgrund „unverhältnismäßigen Aufwands“ (§25 Abs. 2; §30 Abs. 1 Nr. 2; §32 Abs. 1 Nr. 2; §33 Abs. 1 und Abs. 2; §51 Abs. 2; §52 Abs. 3 Nr. 3; §60 Abs. 3 Nr. 3; §65 Abs. 1; §70 Abs. 2 Nr. 3 DSAnpUG-EU-Entwurf) den Schutzcharakter der Vorschriften zur Auskunft und Information von personenbezogenen Daten. Auch die vagen Formulierungen, die statt der Löschung Möglichkeiten in der Einschränkung einer weiteren Verarbeitung personenbezogener Daten vorsehen (§33 Abs. 1; §70 Abs. 2 DSAnpUG-EU-Entwurf), können nicht als grundrechtsfreundliche Alternative bewertet werden. Die zahlreichen Ausnahmetatbestände bei der Wahrnehmung von Betroffenenrechten sind unverhältnismäßig. Auch die angeführten Begründungen für die Einschränkung der Betroffenenrechte, das niedrige Datenschutzniveau liege im öffentlichen Interesse oder sei wichtig für den Schutz der Freiheitsrechte anderer Personen, erscheint mit Blick in die DSGVO abwegig. Eine solche Absenkung des Datenschutzniveaus unter EU-Niveau ist mit dem Recht auf informationelle Selbstbestimmung und dem Grundrecht auf Schutz personenbezogener Daten nach Art. 8 der EU-Grundrechtecharta nicht zu vereinbaren. Das BMI führt in dem Gesetzesentwurf keine Begründungen an, warum Geschäftsinteressen von Auskunfteien schwerer wiegen als Datenschutzrechte betroffener Bürgerinnen und Bürger. Eine solche Fokussierung auf die wirtschaftlichen Interessen im Umgang mit den Betroffenenrechten geht zu Lasten des Persönlichkeitsschutzes und steht der Harmonisierung des Datenschutzes in der Europäischen Union entgegen.

Leider setzt sich hier im nationalen Umsetzungsprozess fort, was schon auf EU-Ebene zu beobachten war: die Aushöhlung des Datenschutzes durch gezieltes Lobbying von Datenhändlern. Den enormen wirtschaftlichen Einfluss verdeutlicht ein Artikel der Süddeutschen Zeitung, nach dem der Europaabgeordnete Louis Michel mehr als 100 Änderungsanträge eingebracht habe, die das Datenschutzniveau tendenziell absenken sollten und nach Recherchen der Plattform „Lobbyplag“ auf Interventionen der Industrie zurückzuführen seien (vgl. SZ vom 25.11.2013, „Ex EU-Kommissar auf schräger Mission“). Insgesamt seien über 3300 Änderungsanträge eingegangen, deren Texte teilweise wörtlich mit denen der Industrie übereinstimmen würden. Die EU-Justizkommissarin Viviane Reding, die den Entwurf zur EU-Datenschutzgrundverordnung vorgelegt hatte, berichtete, dass sie noch nie einen so starken Lobbyeinsatz erlebt habe (Spiegel Online vom 6.6.2013, „Wie die Industrielobby den EU-Datenschutz verwässern will“).

Die Befugnisse der BfDI und der Datenschutzaufsichtsbehörden der Länder müssen nicht abgebaut, sondern deren Kompetenzen und Ressourcen sollten ausgebaut werden. Mindestens jedoch müsste das bestehende Niveau des BDSG gehalten werden, um effektiven Datenschutz im digitalen Zeitalter zu gewährleisten. Mit dem Verweis auf

Vorabfassung - wird durch die lektorierte Fassung ersetzt.

den „Kernbereich exekutiver Eigenverantwortung“ wird die erst im Jahr 2016 mühsam erreichte Unabhängigkeit der BfDI vom Bundesinnenministerium und die Aussagepflicht der BfDI vor Untersuchungsausschüssen und Gerichten beschränkt. Stattdessen müssen endlich effektivere Mittel zur Durchsetzung des Datenschutzrechts gegenüber Behörden und anderen öffentlichen Stellen geschaffen werden, indem Datenschutzverstöße auch dort sanktionsbewehrt werden.

Nicht akzeptabel sind außerdem die Beschränkungen der Prüf- und Berichtsbefugnis im Bereich der Geheimdienste. Vielmehr muss die unabhängige Datenschutzkontrolle der BfDI gegenüber den Nachrichtendiensten verbessert werden. Auch gegenüber den Diensten müssen bußgeldbewehrte Sanktionsmöglichkeiten geschaffen werden.

Ein zentrales Problem der Auskunfteien aus datenschutzrechtlicher Sicht ist die Verwendung personenbezogener Daten zu anderen Zwecken als jenen, zu denen sie zunächst erhoben wurden (Zahlungsabwicklung, Herstellen einer Geschäftsbeziehung). Die Grenzen des auch für den nicht-öffentlichen Bereich geltenden Zweckbindungsprinzips sind unter Datenschützern durchaus umstritten und werden mit jedem neuen Gesetzesvorhaben in diesem Bereich neu gezogen. Problematisch ist weiterhin die unglaubliche Anhäufung von Informationen über große Teile der Bevölkerung, die von Auskunfteien betrieben wird und zu Missbrauch und Manipulation geradezu einlädt. Aus verbraucherschutzpolitischer Sicht ist die intransparente Gewinnung und Gewichtung der Daten problematisch, die schließlich in die prognostische Wertung zur Kreditwürdigkeit bzw. Zahlungsfähigkeit von Kundinnen und Kunden eingehen. Damit ist das Scoring soweit als möglich mit klaren Vorschriften zu beschränken. Zur Durchsetzung dieser Beschränkung muss den Auskunfteien zugleich die Offenlegung der zugrundeliegenden statistisch-mathematischen Modelle von Scoringverfahren auf erlegt werden, die sonst nicht auf grundrechtsrelevante Fragen überprüft werden.

Beim Beschäftigtendatenschutz wurde der alte § 32 BDSG unverändert übernommen, obwohl erhebliche Zweifel angebracht sind, ob die Vorschriften den Vorgaben aus Art. 88 Abs. 2 DSGVO noch entsprechen. Die nationale Reglung sollte „angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz“ (Art. 88 Abs. 2 DSGVO) umfassen. Dies berücksichtigt der Gesetzesentwurf nicht. Sein Regelungsgehalt bezieht sich noch auf eine Welt, in der die einzigen zwischen Unternehmen und abhängig Beschäftigten anfallenden Daten aus der Bewerbungsmappe und der Lohnabrechnung stammten. Dringend erforderlich ist eine Modernisierung des Beschäftigtendatenschutzes, der im Zuge der Digitalisierung der Arbeitswelt eine klare Regulierung für die Erfassung und Verarbeitung von Daten, die im Arbeitsprozess anfallen, benötigt. Diese sollte in einem eigenen Gesetz vorgenommen werden, das auf die derzeit vor allem im Betriebsverfassungsgesetz einschlägigen Regelungen abgestimmt ist.

Vorabfassung - wird durch die lektorierte Fassung ersetzt.